IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

JOHN DOE I and JOHN DOE II, on behalf of themselves and all others similarly situated, Plaintiffs, v. BJC HEALTH SYSTEM d/b/a BJC HEALTHCARE, Defendant.	Case No. 22-cv-00919 Hon. Rodney W. Sippel Electronically Filed

PLAINTIFFS' MOTION TO REMAND AND MEMORANDUM IN SUPPORT

Plaintiffs John Doe I and John Doe II hereby move this Court, pursuant to 28 U.S.C. § 1367, to remand this action to the Twenty-Second Judicial Circuit Court of the City of St. Louis, State of Missouri, in which proper jurisdiction rests.

INTRODUCTION

A. Plaintiffs' Complaint

On July 25, 2022, Plaintiffs filed the underlying Complaint in the Twenty-Second Judicial Circuit Court of the City of St. Louis, State of Missouri, alleging BJC Health System ("BJC") violated its patients' privacy by causing the transmission of their personal and medical information to Facebook, Google, and other third-party marketing companies. BJC's disclosures of patients' personally identifiable data and communications occur through the www.bjc.org and www.barnesjewish.org properties, on the patient portal sign-in page at www.bjc.org/MyChart, and continue even after a patient has identified themselves as a patient by signing-in to the patient portal that BJC falsely claims is a "secure" website for patients. This entire process is invisible to patients and occurs through computer source code BJC secretly deployed that, unbeknownst to patients, commands patient computing devices to transmit patient data to the third parties.

As patients, Plaintiffs have a reasonable expectation of privacy that BJC, their healthcare provider, will not disclose their personal information or the content of their communications exchanged with BJC to third parties for marketing purposes without patient knowledge, consent, or express authorization. Medical providers have a legal and ethical obligation to their patients to keep patient communications, diagnoses, and treatment completely confidential. Patients are aware of the promises of discretion contained within the Hippocratic Oath and must be able to rely on those promises and obligations.

Until now, there was no reason to believe BJC disputed any of this. After all, it expressly and impliedly promised patients that it will maintain the privacy and confidentiality of communications that patients exchange with BJC. For example, BJC promises in its Notice of Privacy Practices that it: (a) is "committed to protecting [patient] health information and to informing [patients] of [their] rights regarding such information"; (b) only "after removing direct identifying information […] from the health information" will BJC potentially use a patient's health information for "research, public health activities or other health care operations (such as business planning), but that BJC will "obtain certain assurances from the recipient of such health information that they will safeguard the information and only use and disclose the information for limited purposes"; (c) "will not engage in disclosures that constitute a sale of [patient] health information without [the patient's] written authorization"; and (d) "will not use or disclose [patient] protected health information for marketing purposes without [the patient's] written authorization."

Plaintiffs brought this action to challenge BJC's practice of secretly transmitting patient data to these social media and data auction companies, alleging breach of fiduciary duty of confidentiality; intrusion upon seclusion; violation of the Missouri Merchandising Practices Act;

Missouri felony computer crimes; and identity theft. No federal jurisdiction exists for Plaintiffs' claims.

B. BJC's Notice of Removal

On September 1, 2022, BJC removed this action pursuant to the Federal Officer Removal Statute, 28 U.S.C. § 1442(a), arguing it was "directed" by the federal government to give its patients' information to Facebook, Google, and other third parties, through its participation in the Promoting Interoperability program.

The Promoting Interoperability program, formerly referred to as the "Meaningful Use Program,"[1] is a voluntary federal program that offers incentive payments to healthcare providers who meet certain program requirements. There are no requirements for hospitals in the Promoting Interoperability programs to show actual patient engagement with any EHRs or patient portals. Instead, to qualify for the voluntary incentive interoperability program, hospitals like BJC are only *required* to "protect patient health information" and to earn a total of 60 points from the following categories:

a. Engage in e-prescribing – For this category, a provider can earn up to 20 points in 2022, with 10 of those points dependent upon adopt of a prescription drug monitoring program measure to Schedule II opioids.[2]

[1] In 2018, the official name of the "meaningful use" program was changed from the "Medicare and Medicaid EHR Incentive Programs" to the "Medicare and Medicaid Promoting Interoperability (PI) Programs." The Centers for Medicare & Medicaid Services ("CMS") explained that the name-change referred to the increased "focus of EHR reporting on interoperability and sharing data with patients." 83 FR 201518.

[2] 42 C.F.R. § 495.24(e)(5), (e)(5)(iii)(B)

b. Exchange health information with other providers when transitioning or referring their patient to another setting of care using EHR and CEHRT – For this requirement, a provider can earn up to 40 points.[3]

c. Provide patients with timely electronic access to their health information – For this requirement, a provider can earn up to 40 points.[4]

d. Actively engage with a public health agency or clinical data registry to submit electronic public health data using CEHRT – For this requirement, a provider can earn up to 15 points.[5]

42 C.F.R. § 495.24(e), *Stage 3 Objectives and Measures for Eligible Hospitals and CAHs Attesting to CMS for 2022.*

BJC's Notice of Removal argues that its choice to voluntarily enroll in the Promoting Interoperability program—which was designed to encourage the use and safeguarding of patient electronic medical records—somehow constituted federal permission to disclose patient information to Facebook and Google for marketing purposes. Also, BJC argues that it has a First Amendment right to give its patients' personal and health information to Facebook and Google. BJC's removal is as shocking as it is unfounded, and this matter should be remanded.

THE FEDERAL OFFICER REMOVAL STATUTE, 28 U.S.C. § 1442

In pertinent part, the federal officer removal statute provides that a civil action may be removed to federal court where the action is against or directed to "[t]he United States or any agency thereof or any officer (or any person acting under that officer) of the United States or of any agency thereof, in an official or individual capacity, for or relating to any act under color of

[3] 42 C.F.R. § 495.24(e)(6)
[4] 42 C.F.R. § 495.24(e)(7)
[5] 42 C.F.R. § 495.24(e)(8)

such office[.]" 28 U.S.C. § 1442(a)(1). To fall within the purview of § 1442(a)(1), a Defendant must show that (1) it acted under the direction of a federal officer, (2) there is a causal connection between its actions and the official authority, (3) it has a colorable federal defense to the plaintiffs' claims, and (4) it is a "person," within the meaning of the statute. *Buljic v. Tyson Foods, Inc.*, 22 F.4th 730, 738 (8th Cir. 2021). The removing party bears the burden of proving the grounds supporting federal officer removal. *See, e.g., Ruppel v. CBS Corp.*, 701 F.3d 1176, 1180 (7th Cir. 2012).

The "basic purpose" of the Federal Officer Removal Statute, 28 U.S.C. § 1442, "is to protect the Federal government from the interference with its operations" and to ensure that federal officials have an appropriate forum to assert federal immunity defenses. *Watson v. Phillip Morris Cos., Inc.*, 551 U.S. 142, 150 (2007).

The Eighth Circuit has explained that "not all relationships between private entities and the federal government satisfy" the element of acting under the direction of a federal officer. *Buljic*, 22 F.4th at 738. "[T]he fact that a regulatory agency directs, supervises, and monitor's a company's activities in considerable detail" does not make the company one acting under a federal officer. *Watson v. Phillip Morris Cos., Inc.*, 551 U.S. 142, 145 (2007). Furthermore, "[t]he fact that an entity […] is subject to pervasive federal regulation alone is not sufficient to confer federal jurisdiction. This is so because '[a] private firm's compliance (or non-compliance) with federal laws, rules, and regulations does not itself fall within the scope of the statutory phrase 'acting under' a federal 'official.'" *Buljic*, 22 F.4th at 739 (quoting *Watson*, 551 U.S. at 153) (citing *Jacks*, 701 F.3d at 1230 ("It is not enough that a private person or entity merely operate in an area directed, supervised and monitored by a federal regulatory agency or other such federal entity.")). "Instead,

the private entity must help federal officers fulfill basic *governmental tasks*." *Buljic*, 22 F.4th at 739 (citation omitted) (emphasis added).

The Supreme Court has further explained that federal officer removal applies "only if [the private person was] *authorized* to act *with or for* federal officers are agents in affirmative executing duties under federal law" and to private persons "who *lawfully* assist" the federal officer "in the performance of his official duty." *Watson v. Phillip Morris Cos., Inc.*, 551 U.S. 142, 151 (2007).

ARGUMENT

Plaintiffs do not dispute that BJC is a "person" as defined in the statute. However, BJC otherwise fails to establish that (1) it acted under the direction of a federal officer, (2) there is a causal connection between its actions and the official authority, or (3) it has a colorable federal defense to Plaintiffs' claims.

BJC's sole affirmative argument for removal under the Federal Officer Removal Statute is based on its voluntary participation in the Promoting Interoperability program which provides BJC with financial rewards that encourage healthcare providers to do what they should already have been doing. Namely, protect patient privacy and utilize electronic medical records intended to enhance patient safety and healthcare portability. But to be clear, *BJC's Notice of Removal fails to identify any bequest of a federal officer or agency requesting BJC disclose patient data to Facebook, Google, and any other third party identified in Plaintiffs' Complaint*.

A. BJC Fails to Establish the "Acting Under" Element

To come within the scope of the Federal Officer Removal Statute, BJC must establish it is acting under the direction of a federal officer with respect to the conduct at issue in Plaintiffs' Complaint. *Watson v. Philip Morris Companies, Inc.*, 551 U.S. 142, 147 (2007). BJC contends

that it is acting under a federal official because it created an online patient portal as part of its participation in the Promoting Interoperability program.

A private actor such as BJC acts under the direction of a federal officer or agency when it helps fulfill "basic governmental tasks" that the federal Government would otherwise have to provide itself. *Buljic v. Tyson Foods, Inc.*, 22 F.4th at 739. For instance, courts have found that providing health insurance to federal employees, representing indigent federal defendants, and contracting with the Government to provide a product are instances of "acting under" federal officials. *Id.* In contrast, BJC's creation of its online patient portal does not constitute a "basic governmental task" that the Government would have otherwise carried out for BJC. In fact, BJC could qualify for the "higher federal payments" under the Promoting Interoperability program without having a patient portal at all because there are at least 75 points available for CEHRT interoperability measures that have nothing to do with electronic health records. At most, the Government encouraged BJC to participate in the Promoting Interoperability program, but it did not direct BJC to do so—and the Government certainly did not direct BJC to create a patient portal as part of its participation. *Buljic*, 22 F.4th at 741 (citing *Mays v. City of Flint*, 871 F.3d 437, 446-47 (6th Cir. 2017) (absent a federal order to take specific action during the Flint water crisis, the City of Flint could not satisfy the acting under element)). BJC's voluntary participation in the program falls well short of demonstrating the type of "subjection, guidance, or control" or legal delegation of authority that is necessary to show BJC was "acting under" a federal official. *Watson*, 551 U.S. at 147.

Further, even though BJC's participation in the voluntary program may be related to an important national infrastructure, "the fact that an industry is considered critical does not necessarily mean that ever entity within it fulfills a basic governmental task[.]" *Buljic*, 22 F.4th at

740; *see Cagle v. NHC HealthCare-Maryland Heights, LLC*, No. 4:21CV1431 RLW, 2022 WL 2833986, at *2 (E.D. Mo. July 20, 2022) (finding removal under the Federal Officer Removal Statute not warranted where the defendant nursing home argued the plaintiff's complaint related to the defendant's compliance with COVID-19 regulations and directives as part of nursing home's designation as a "critical infrastructure of the United States").

Finally, BJC's interpretation of the Federal Officer Removal Statute's "acting under" requirement stretches the Statute far from its original purpose. A state-court lawsuit that prevents BJC from sending its patients' information to Facebook and Google surely would not interfere with Government operations. Additionally, BJC is not at risk of state-court prejudice because it created an online patient portal and BJC would not be denied its ability to assert a federal claim of immunity. *See Watson*, 551 U.S. at 150.

In sum, BJC was not "acting under" a federal official when it created its online patient portal. BJC's creation of its online patient portal is not a "basic" governmental task that the Government would have performed for BJC and BJC cannot point to any directive that required it create its portal. BJC's voluntary participation in a federal incentive program is not the type of relationship with a federal official necessary to support Federal Officer Removal jurisdiction.

B. BJC Fails to Establish the Causation Element

Even if BJC's participation in the Promoting Interoperability program could satisfy the "acting under" element, BJC fails to establish a causal connection between the complained-of conduct and the asserted official authority. BJC's Notice of Removal glosses over an obvious and fatal flaw in its alleged basis for removal—this case has nothing to do with BJC's participation in the program. Rather, this case is about BJC's breach of basic Missouri common law, statutory, and contractual duties to Plaintiffs and other patient members of the putative class as a result of BJC's

transmission of patient communications to third parties. No federal jurisdiction exists to justify the removal of this action.[6]

BJC attempts to avail itself of the Federal Officer Removal Statute under the general auspices of participating in the Promoting Interoperability program. But this is insufficient to evoke federal jurisdiction "in the same way a bona fide federal officer could not remove a trespass suit that occurred while he was taking out the garbage." *3M*, 17 F.4th at 769. Instead, BJC must establish a causal connection between its purported authority to promote healthcare interoperability and sending patient communications to Facebook, Google, and other third parties. *See Watson*, 551 U.S. at 147 ("The federal statute permits removal only if [the defendant], *in carrying out the 'acts' that are the subject of the petitioners' complaint*, was 'acting under' any 'agency' or 'officer' of 'the United States.'") (emphasis added); *In re Guidant Corp. Implantable*

[6] Courts in this district have previously rejected BJC's attempt to remove a complaint alleging state law claims merely because those claims implicated federal statutes. For example, in *Alade v. Barnes-Jewish Hosp., Inc.*, No. 4:12-CV-497 CAS, 2012 WL 2598091, at *4 (E.D. Mo. July 5, 2012), the court rejected BJC's attempt to remove under § 1331, concluding that:

> Although plaintiff's Petition makes multiple, specific reference to federal statutes USERRA and EMTALA, and alleges that defendant Farber and BJH showed hostility towards plaintiff's military career, *the underlying causes of action do not arise under USERRA or EMTALA within the meaning of 28 U.S.C. § 1331. None of plaintiff's claims include a federal cause of action under either USERRA or EMTALA. All counts of the Petition assert state law claims*. The Petition's references to alleged violations of USERRA and EMTALA by the defendants are part of the factual background to plaintiff's assault, battery, false imprisonment, and other state law claims.

(emphasis added). The same is true in this case. Plaintiffs' claims arise solely under state law and merely refer to HIPAA to provide background on BJC's duty to protect patient privacy. Of course, HIPAA is not necessary for the prosecution of Plaintiffs' claims against BJC *at all* because BJC's portal partner adopted HIPAA's definition of PHI in its own internal policies. Thus, even to the extent HIPAA is implicated in Plaintiffs' claims it is merely duplicative of the identical duty BJC assumed through written privacy promises.

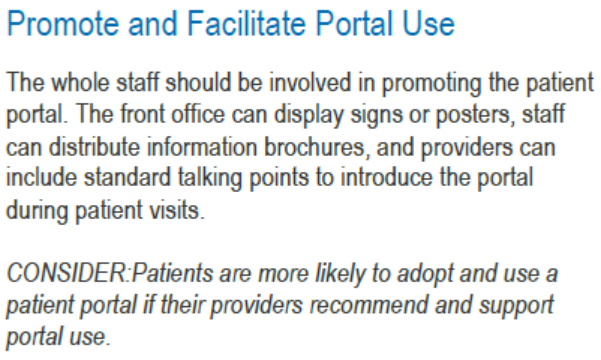
Defibrillators Prod. Liab. Litig., 428 F. Supp. 2d 1014, 1018 (D. Minn. 2006) (finding the Federal Officer Removal Statute did not apply where there the defendant did "not contend that the FDA directed the design, manufacture, or marketing of the defibrillators at issue in a manner that gave rise to the defects and deception alleged in Plaintiffs' complaints"); *see also Arness v. Boeing N. Am., Inc*., 997 F. Supp. 1268, 1273-75 (C.D.Cal.1998) (Federal Officer Removal Statute did not apply in a case alleging improper disposal of a toxic substance where the government required that a contractor use the toxic substance, but the government did not specify how the defendants should have disposed of the cleanser); *Faulk v. Owens-Corning Fiberglass Corp.*, 48 F. Supp. 2d 653, 664 (E.D. Tex. 1999) (corporation that produced products under government specifications could not avail itself of the Federal Officer Removal Statute in a case involving failure to warn because the government "remained completely silent as to whether to *warn* about the use of asbestos").

The Promoting Interoperability program does not require or even suggest the disclosure of patient information to third parties for advertising purposes. To the contrary, all of the federal officers and agencies BJC scapegoats for its own privacy violations have encouraged medical providers to adopt technologies that *protect* the privacy and security of patient data. There is no rule or regulation mandating that a hospital share patient personally identifiable data with third parties in order to increase patient knowledge and use of a hospital website or patient portal. Nor is there anything in the "meaningful use" requirements that repeals HIPAA or any state privacy law that is more protective of privacy than HIPAA.

The "meaningful use" programs cited by BJC have gone through at least four significant substantive rounds of rulemaking. In every round, the federal government has indicated that "protecting patient privacy" is a core objective. In Stages Two and Three and the current rule, protecting patient privacy was the federal government's *first* objective. As ONC has explained,

"Protecting patients' privacy and securing their health information stored in an EHR is a core requirement of the Medicare and Medicaid EHR Incentive Programs." *See* "Guide to Privacy and Security of Electronic Health Information, Office of the National Coordinator for Health Information Technology", available at: https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Nor does BJC identify any rule, statement, or communication from any federal agency or officer that could be deemed as a requirement or encouragement to use Facebook, Google, and other third-party marketing tools in connection with data about patients absent full disclose and consent.

BJC's only arguments concerning the federal government's "authorization" of its use of Facebook, Google, and other third-party source code on its website actually support Plaintiffs' claims. *First*, BJC relies on a fact sheet published by the Office of the National Coordinator for Health Information Technology as "specif[ing] how providers can optimize such portals; 'how a patient portal helps achieve meaningful use requirements'; and how a provider can 'actively promote and facilitate portal use.'" Def. Not. at ¶21. This is true. The ONC does specifically state how portals should be promoted. Unfortunately for BJC, the ONC states that portal should be promoted—not through channels that provide patient information to Facebook and Google—but by in-person interactions:



Promote and Facilitate Portal Use

The whole staff should be involved in promoting the patient portal. The front office can display signs or posters, staff can distribute information brochures, and providers can include standard talking points to introduce the portal during patient visits.

CONSIDER:Patients are more likely to adopt and use a patient portal if their providers recommend and support portal use.

> To simplify the portal registration process, have staff assist patients with the process, and consider providing a registration kiosk in the office. Staff can educate patients about how to use the portal's features, and can offer guidance about the kinds of communication that are appropriate between providers and patients.

ONC, How to Optimize Patient Portals for Patient Engagement available at https://www.healthit.gov/sites/default/files/nlc_how_to_optimizepatientportals_for_patientengagement.pdf. Nothing in ONC's guidance directs BJC to transmit patient information to Facebook and Google in order to promote portal use. As a result, the fact does not assist BJC in meeting its burden on removal.

Then BJC makes the wholly unfounded claim that CMS's patient portal "offer[s] a model for private providers to follow." Def. Not. at ¶ 22. Of course, BJC cites no authority for the idea that CMS designed its portal to be used as a template for private providers. Nor does BJC cite any evidence demonstrating that it designed its own website and portal based on the example provided by the CMS website. To the contrary, we know beyond a doubt that *BJC did not use the CMS website as a template* for its own web property because BJC appears to have completely ignored all of the material disclosures CMS included in its privacy policy.

CMS includes a detailed 14-page privacy policy on its website that BJC admits discloses the use of Google and Facebook marketing tools. Exhibit A. On the other hand, BJC does—and couldn't—claim that it made any of these same disclosures to its own patients. Instead, BJC's privacy policy is little more than one page and over half of which is dedicated largely to lawyerly language discussing copyright and intellectual property rights. Exhibit B. Most importantly, BJC makes no mention of its use of Facebook, Google, or any other third-party tools anywhere in the policy. Nor does it disclose the transmission of any PII to these third parties. Furthermore, the

CMS website provides specific instructions on how patients can opt out of the third-party tools which BJC doesn't even acknowledge, let alone give patients the ability to avoid.

So taking BJC's argument as face value, the only thing it has proven is that (1) it was aware of the CMS website (which BJC appears to consider "best practice"), and (2) it completely ignored all of its privacy disclosures while nonetheless utilizing all of the third party tools on the CMS website and then some. This falls well short of BJC's burden to show that a federal officer authorized it to share patients' information with Facebook and Google.

C. BJC Does Not Present a Colorable Federal Defense

"To qualify for removal, a defendant must, among other things, raise 'a colorable defense arising out of [the defendant's] duty to enforce federal law.'" *U.S. v. Todd*, 245 F.3d 691 (8th Cir. 2001) (quoting *Mesa v. California*, 489 U.S. 121, 133, 109 S.Ct. 959 (1989)). A "colorable federal defense must be something more than a desire to protect a generalized federal interest or to encourage a preferred interpretation of federal law in a dispute between private parties." *Guggenberger v. Starkey Laboratories, Inc.*, 2016 WL 7479542, at *11 (D. Minn. Dec. 29, 2016). "Innumerable state-court proceedings affect federal interests, *including every proceeding in which a court must interpret and apply a federal statute or regulation*." *Id*. (quoting *Peoples Nat'l Bank of Mora v. BWHC, LLC*, 2008 WL 10973336, at *4 (D. Minn. Oct. 10, 2008) (emphasis added). "[I]t is the Defendants' burden to demonstrate a colorable defense" and "not 'the mere possibility of some future evidence as the basis for removal.'" *Minnesota v. American Petroleum Institute*, 2021 WL 1215656, at *9 (D. Minn. March 31, 2021) (quoting *Graves v. 3M Co.*, 447 F.Supp.3d

908, 916 n. 8 (D. Minn. 2020)). Partial defenses are not sufficient to invoke federal officer removal. Fact defenses are not sufficient to invoke federal officer removal.

BJC's Notice of Removal claims to have "at least two colorable federal defenses": the first being under HIPAA, which "turns on an interpretation of federal law", and the First Amendment, specifically that the First Amendment permits BJC to disclose patients' information to Facebook, Google, and others. BJC DNR ¶¶ 37-40. Neither defense has any merit.

First, Plaintiffs do not dispute that HIPAA is implicated in their claims. HIPAA is pled as one of many sources of the duties that BJC owes to its patients. However, *compliance* with HIPAA does not constitute a defense to any of Plaintiffs' claims for two reasons. *First,* HIPAA does not preclude state law causes of action for the disclosure of patient information. That is, even if a fact finder found that BJC had fully complied with HIPAA—which it didn't—it still would not preclude liability under *any* of Plaintiffs' state law causes of action because they are "more stringent" privacy protections. 45 C.F.R. § 160.203(b). Rather, HIPAA's role in this case is to merely inform Defendant's duties—it does not provide the legal *defense* for any cause of action.

For these reasons, courts in this district have routinely granted motions to remand under similar situations where HIPAA is pled as the standard of care for negligence *per se* claims and the defendant removed under federal question jurisdiction. For example, in *I.S. v. Washington Univ.*, No. 4:11CV235SNLJ, 2011 WL 2433585, at *5 (E.D. Mo. June 14, 2011), the plaintiff sued Washington University, alleging it disclosed her appointment information to a third party without her authorization. Washington University removed the matter to federal court, arguing that the plaintiff's reliance on the underlying HIPAA violation for her negligence *per se* claim raised a federal question. However, citing numerous cases in this district, the court disagreed, finding that "plaintiff's claim for 'negligence *per se*' … does not raise any compelling federal interest nor is a

substantial federal question presented. Although HIPAA is clearly implicated in the claim for negligence *per se*, said claim falls within that broad class of state law claims based on federal regulations in the state court."

Defendant's argument here is even weaker than that rejected in *I.S.* In that case, HIPAA was the *entire basis* for the negligence *per se* claim and, presumably, a successful defense to the regulatory violation may have precluded liability. Here, Plaintiffs' claim relies far more than HIPAA alone, including:

a. BJC's status as Plaintiffs' health care provider;

b. BJC's common law obligation to maintain the confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communications and computer data;

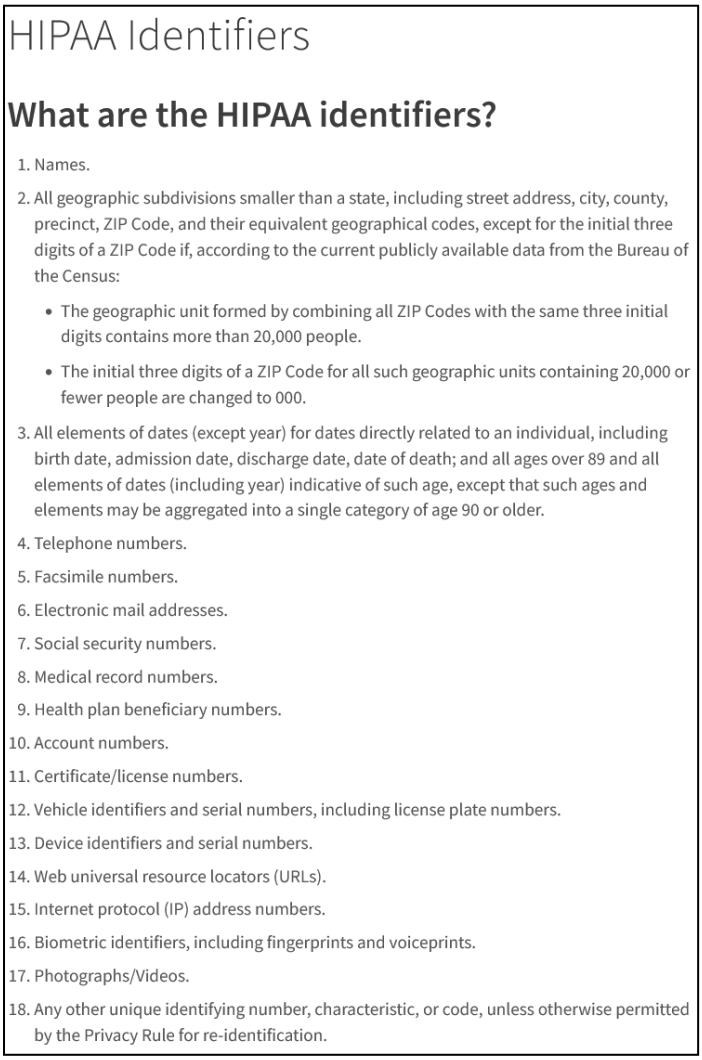
e. State laws protecting unauthorized use of personal means of identification;

f. Defendants' express promises of confidentiality; and

g. Defendants' implied promises of confidentiality.

Petition ¶18. Furthermore, Defendant's position overstates the rigors of analysis of HIPAA required by its position. There is no "interpretation" of HIPAA at issue in this case. HIPAA was specifically drafted to avoid the need for such "interpretation" by clearly defining PII to explicitly include geo-location information, medical record numbers, account numbers, device identifiers, URLs, IP addresses, and any "other unique identifying number, characteristic, or code." Petition,

¶49. 58, 63, 77. This is undisputed. In fact, Defendants' portal co-owner, Washington University Physicians, *adopts* the HIPAA definition of PII:



HIPAA Identifiers

What are the HIPAA identifiers?

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
   - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
   - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Photographs/Videos.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

HIPAA Identifiers, Washington University in St. Louis, https://hipaa.wustl.edu/resources/hipaa-identifiers/ (last visited July 15, 2022); Petition, ¶49. Moreover, BJC's privacy policy explains its "duties regarding your health information" in its privacy notice, stating:

OUR DUTIES REGARDING YOUR HEALTH INFORMATION

We respect the confidentiality and personal nature of your health information. We are committed to protecting your health information and to informing you of your rights regarding such information. We are required by law to protect the privacy of your protected health information, to provide you with notice of these legal duties and to notify you following a breach of unsecured protected health information. This Notice explains how, when and why we typically use and disclose health information and your privacy rights regarding your health information. In our Notice, we refer to our uses and disclosures of health information as our "Privacy Practices." Protected health information generally includes information that we create or receive that identifies you and your past, present or future health status or care or the provision of or payment for that health care. We are obligated to abide by these Privacy Practices as of the effective date listed below.

Thus, there is no disagreement before the court on HIPAA's requirements because HIPAA and Defendant use the same definition and BJC agrees that it is "required by law to protect the privacy of [patient] protected health information." Furthermore, since compliance with HIPAA would not defeat any claims, it cannot be a basis for federal jurisdiction.

Next, BJC shockingly claims that it has a First Amendment right to disseminate patient information to Facebook and Google over the Internet. *First*, BJC—a trusted healthcare provider in the community—does not have a First Amendment right to "disseminate" its patients' medical information to *anyone* let alone Facebook and Google. It is (or should be) beyond dispute that "HIPAA prohibits the wrongful disclosure of individually identifiable health information." *In re Bextra & Celebrex Mktg., Sales Pracs. & Prod. Liab. Litig.*, No. 4:07MC00309 CEJ, 2007 WL 2030243, at *2 (E.D. Mo. July 10, 2007). This is not a novel concept and is explicitly incorporated in BJC's privacy policy. Furthermore, BJC's right to transmit patient data to Facebook and Google cannot be reconciled with the federal government's effort to preserve patient privacy through the Promoting Interoperability program. Indeed, BJC's entire removal argument, taken together, appears to be that federal officer removal is warranted due to its compliance with a federal incentive and privacy-preserving program that unconstitutionally infringes on its First Amendment right to transmit patient data to Facebook and Google for its own financial gain.

Second, every federal appellate court to consider a First Amendment challenge to HIPAA has flatly rejected the defense. *South Carolina Med. Ass'n v. Thompson*, 327 F.3d 346, 355 n. 4 (4th Cir.2003) ("summarily dispens[ing]" with a First Amendment challenge in a single sentence footnote, finding it "without merit"); *Citizens for Health v. Leavitt*, 428 F.3d 167, 184–85 (3d Cir. 2005) (finding "a First Amendment claim is an ill-suited challenge to the [HIPAA's] Amended Rule."). Thus, while BJC may believe that HIPAA's prohibitions against selling patient personal and medical information to Facebook and Google are unconstitutional, federal courts do not.

But perhaps this is why BJC's only support for its First Amendment defense comes from a case that had nothing to do with *patient* information. In *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011), the Supreme Court struck down a Vermont law which precluded the dissemination of information that identified the *prescribing habits of doctors.* That is, *Sorrell* specifically and exclusively concerned pharmacies receiving "*prescriber*-identifying information" when processing prescriptions and selling the *prescriber's information* to "data miners," who in turn produced reports on the *prescriber's behavior* for pharmaceutical manufacturers. Notably, the prescribing information at issue in *Sorrell* did not include *any patient* information. Therefore, nothing in *Sorrell* addresses—let alone permits—doctors to disclose patient information for marketing purposes.

Taken together neither HIPPA nor the First Amendment provide any defense, let alone a colorable defense, to any of Plaintiffs' claims.

CONCLUSION

WHEREFORE, Defendant BJC has failed to meet its burden showing that the Federal Officer Removal Statute, 28 U.S.C. § 1442(a), applies here, Plaintiffs John Doe I and John Doe II respectfully request that this Court grant their Motion to Remand and that this action be remanded

to the Twenty-Second Judicial Circuit Court of the City of St. Louis, State of Missouri, in which proper jurisdiction rests.

Dated: October 3, 2022

Respectfully submitted,

THE SIMON LAW FIRM, P.C.

By: *Elizabeth S. Lenivy*
Elizabeth S. Lenivy #68469
Amy Collignon Gunn #45016
800 Market Street, Ste. 1700
St. Louis, MO 63101
Phone: (314) 241-2929
Fax: (314) 241-2029
elenivy@simonlawpc.com
agunn@simonlawpc.com

SIMMONS HANLY CONROY LLC

Jason 'Jay' Barnes #57583
Eric Johnson #61680
112 Madison Avenue, 7th Floor
New York, NY 10016
Phone: (212) 784-6400
Fax: (212) 213-5949
jaybarnes@simmonsfirm.com
ejohnson@simmonsfirm.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of October 2022, a true and correct copy of the foregoing was electronically filed with the Clerk of Court and served to all counsel of record via the Court's CM/ECF system.

/s/ Elizabeth S. Lenivy